TAICS

TAICS TS-0045 v1.0 : 2021

# 消費性物聯網產品資安標準

# Cybersecurity standard for consumer IoT products

2021 / 11 / 25

社團法人台灣資通產業標準協會
Taiwan Association of Informationand Communication Standards

# 消費性物聯網產品資安標準

# Cybersecurity standard for consumer IoT products

出版日期: 2021/11/25

終審日期: 2021/11/19

# 誌謝

本標準由台灣資通產業標準協會－TC5 網路與資訊安全技術工作委員會所制定。

TC5 主席：神盾股份有限公司 張心玲 副總經理

TC5 副主席：財團法人資訊工業策進會 毛敬豪 資安鑄造廠總經理

TC5 副主席：財團法人資訊工業策進會 蔡正煜 主任

TC5 副主席：財團法人電信技術中心 林炫佑 副執行長

TC5 物聯網資安工作組組長：財團法人資訊工業策進會 高傳凱 副主任

技術編輯：財團法人資訊工業策進會 賴怡伶 工程師

財團法人電信技術中心 王慶豐 副主任、許博堯 副理

此標準制定之協會會員參與名單為(以中文名稱順序排列)：

大同股份有限公司、中華資安國際股份有限公司、中華電信股份有限公司、中興保全科技股份有限公司、友達光電股份有限公司、台灣是德科技股份有限公司、台灣惠普資訊科技股份有限公司、台灣德國萊因技術監護顧問股份有限公司、台灣檢驗科技股份有限公司、安華聯網科技股份有限公司、行動檢測服務股份有限公司、尚承科技股份有限公司、神盾股份有限公司、財團法人工業技術研究院、財團法人資訊工業策進會、財團法人電信技術中心、國立陽明交通大學、國家中山科學研究院、勤業眾信聯合會計師事務所、遠傳電信股份有限公司

本計畫專案參與廠商(法人)名單為(以中文名稱順序排列)：

友訊科技股份有限公司、天主教輔仁大學、行政院消費者保護處、財團法人中華民國消費者文教基金會、國立雲林科技大學、國立臺灣科技大學

本標準由國家通訊傳播委員會支持研究制定。

# 目錄

# 前言

本標準係依台灣資通產業標準協會(TAICS)之規定，經理事會審定，由協會公布之產業標準。

本標準並未建議所有安全事項，使用本標準前應適當建立相關維護安全與健康作業，並且遵守相關法規之規定。

本標準之部分內容，可能涉及專利權、商標權與著作權，協會不負責任何或所有此類專利權、商標權與著作權之鑑別。

# 引言

有鑑於消費性物聯網產品已逐漸普及應用於日常生活，根據IEK的「物聯網資安威脅與解決方案發展方向」[(1)]研究報告中指出，七大高風險遭駭客攻擊之物聯網裝置排行中(七大高風險物聯網裝置：家用網路路由器、電視盒、智慧家居產品、植入式醫療裝置、關鍵基礎設施、嬰兒監視器及連網汽車)，就有四種屬於消費性物聯網產品(家用網路路由器、機上盒、智慧家居產品、嬰兒監視器)，消費性物聯網產品相對安全防護能力更加不足，資安問題屢見不鮮，卻未有較明顯且具體的改善。因此在國家通訊傳播委員會的支持下，以 ETSI EN 303 645 Cyber Security for Consumer Internet of Things：Baseline Requirements[1]為基礎，並符合國內消費性物聯網產業之產品實際現況，以建構可檢測之資安指引為目的，制定我國消費性物聯網產品資安產業標準，作為消費性物聯網產品資安品質要求之依據。

# 1. 適用範圍

本標準規定消費性物聯網產品之資訊安全要求。消費性物聯網產品為透過與關聯服務所連接的連網設備，但關聯服務不在本適用範圍內，其相關應用包括但不限於智慧家庭與人身穿戴應用之消費性物聯網產品，例如：

(a) 具有連網功能之家庭電器產品：可連網冰箱、可連網電視等。

(b) 人身穿戴應用：智慧手環等；智慧手錶不在本適用範圍內。

本標準的適用範圍涵蓋消費性物聯網應用設備及其連接之無線網路環境，如下圖 1 所示：

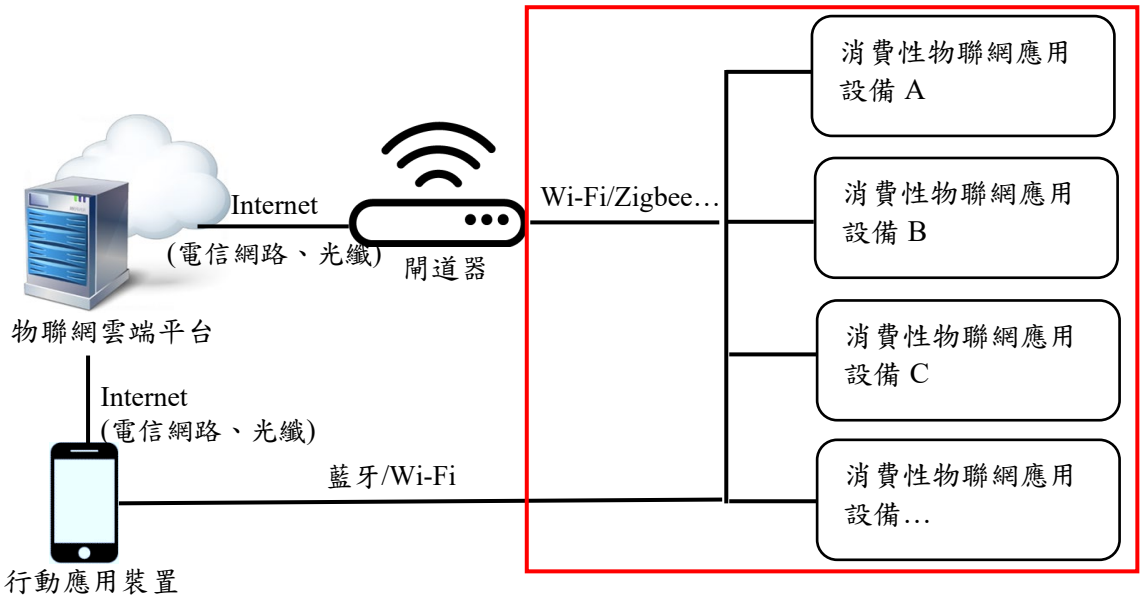


圖 1 適用範圍示意圖

# 2. 引用標準

下列標準因本標準所引用，成為本標準之一部分。有加註年份者，適用該年份之版次，不適用於其後之修訂版(包括補充增修)。無加註年份者，適用該最新版(包括補充增修)。

[1] ETSI EN 303 645 V2.1.1 (2020-06) Cyber Security for Consumer Internet of Things: Baseline Requirements

# 3. 用語及定義

下列用語與定義適用於本標準。

## 3.1 消費性物聯網產品(Consumer IoT products)

指消費性物聯網產品用於消費者可自行安裝設置或穿戴之連網設備，透過無線傳輸技術與關聯服務相互整合，消費者可監看與遙控消費性物聯網產品。例如：包括但不限於智慧家電、家庭閘道器、智慧手環等產品。

## 3.2 受限制設備 (Constrained device)

為此類設備預期用途受限於實體而產生的限制，包括但不限於處理資料的能力、通訊的能力、資料儲存的能力或與使用者互動的能力。例如感測器，它可能是(1)實體限制的設備，可能因電源、電池壽命、運算處理能力、實體的存取、功能有限、記憶體有限或網路頻寬有限，這些限制在設備運行時可能需要搭配另一設備來支援；或(2)可能是透過同一實體線路供電與資料傳輸，此設備的通訊協定與加密方式就受限於該線路配置。

## 3.3 關聯服務 (Associated services)

指消費性物聯網產品提供的產品功能所需的數位服務，包括行動應用程式(App)、雲服務(雲端運算、雲端儲存)、第三方 API 及傳輸遙測數據的第三方服務等。

## 3.4 遙測數據 (Telemetry data)

指來自產品的資訊，可以提供廠商用以識別問題或改善產品服務所需之相關的訊息，例如：包括但不限於故障回報、GPS 定位座標、使用習慣紀錄等資訊。

## 3.5 個人資料 (Personal data)

係指對於已識別或可識別自然人有關的任何資訊，包括識別個人身分之隱私資料，例如：身分證字號、電話號碼、住址、車牌及生物辨識相關之影像等。

### 3.6 敏感性個人資料 (Sensitive personal data)

此類之個人資料遭洩露後可能對個人權益造成損害，此類資料統稱為「敏感性個人資料」。例如:家用網路攝影機之影像串流、付款資訊、帶有時間戳記的人身定位資料、身分 ID 等。

### 3.7 關鍵安全參數 (Critical security parameter)

係指與安全相關的資料(例如:機密資訊、金鑰)及身分驗證資料（例如:通行碼、PIN 碼），當此資料被揭露或修改時，可能會損害密碼模組的安全性。例如：產品透過 OTA 更新韌體時，當更新伺服器發送之憑證金鑰遭惡意人士竄改或擷取，可能造成更新失敗或韌體遭竊取。

### 3.8 敏感性安全參數 (Sensitive security parameters)

係指包括關鍵安全參數以及與安全性相關的公共資訊，例如:用於驗證軟體更新的真確性和完整性的公鑰。

### 3.9 持久性儲存器 (Persistent storage)

指此類的儲存設備所儲存的任何資料，在該設備電源關閉後資料仍會保存。亦稱為非揮發性記憶體(Non-volatile storage)，例如:唯讀記憶體(ROM)、快閃記憶體(flash)、硬碟(hard disk)等。

### 3.10 國家弱點資料庫 (National vulnerabilities database)

指美國國家標準技術研究所(National Institute of Standards and Technology, NIST)提供的國家弱點資料庫[5]，負責常見弱點與漏洞(如 3.5 所述)之資料的發布及更新。

### 3.11 常見弱點與漏洞 (Common Vulnerabilities and Exposures, CVE)

由美國國土安全部贊助之弱點管理計畫，針對每一弱點項目給予全球認可之唯一共通編號。

## 3.12 通用漏洞評分系統 (Common Vulnerability Scoring System, CVSS)

由資安事件應變小組論壇(Forum of Incident Response and Security Teams, FIRST) 提供的漏洞評分系統[7]，目前發展至第 3 版，以衡量軟體漏洞的特徵和嚴重性進行評分。

## 3.13 管理者 (Administrator)

具更改產品設定、作業系統、控制介面、功能應用程式之權限人員，如系統管理者。

## 3.14 通行碼 (Password)

指一組能讓消費者使用系統或以識別消費者身分之字元串，包括本機儲存資料加密檔案密碼、自身帳號及密碼、遠端網路服務帳號及密碼。

## 3.15 預設通行碼 (Default password)

指產品出廠預先設定好的通行碼，即消費者在初次將其連上網路，且在未更改任何設定的情況下，用以登入產品之通行碼。

## 3.16 加密 (Encryption)

指為了避免資訊的洩漏，明文資訊透過數學演算法進行改變，使原來的明文資訊變成不可讀而達到保密之目的。

## 3.17 安全事件 (Security event)

本標準之安全事件定義為，包括但不限於消費者登入、配置設定之各種可能發生威脅或攻擊事件之活動。

## 3.18 安全通道 (Security tunnel)

為網際網路通訊端點與端點(End-to-End)間，並達到資料隱密性及完整性所建立之通道，如：目前常見之實作安全套接層協定 (Secure Sockets Layer, SSL)和傳輸層安全性(Transport Layer Security, TLS)。

## 3.19 前向安全 (Forward Secrecy, FS)

指萬一通行碼或金鑰在某個時間點不慎洩漏，過往的通訊依然是安全，不會因此而洩漏過去的通訊數據。

## 3.20 安全更新 (Security update)

指修復廠商自行發現或使用者回報之產品安全漏洞的軟、韌體更新。

## 3.21 無線下載 (Over-the-air, OTA)

為一種裝置透過行動網路、Wi-Fi 等無線傳輸，下載更新韌體並自動安裝的技術。

## 3.22 網路埠 (Port)

網路埠，又稱為通訊埠或者連接埠，作為連網裝置與外部來源之間傳送/接收通訊資料的端口。

# 4. 安全構面與要求

本標準為消費性物聯網產品之網路安全要求，所有安全要求項目皆參照 ETSI EN 303 645 消費性物聯網產品之基本要求。

## 4.1 安全構面與要求概述

安全構面與要求總表如表 1 所示，第一欄為安全構面，包括：(1)身分鑑別、(2)漏洞安全、(3)軟韌體更新、(4)資料機密性與完整性、(5)系統完整性、(6)資源可用性、(7)隱私保護及(8)異常與警示；第二欄為安全要求，係依第一欄安全構面設計之對應安全要求；第三欄為安全層級與條件；第四欄為安全要求項目，須依循第 5 節之技術規範內容。其中，關於第三欄安全層級與條件之說明，如下所述：

(a) 第三欄之安全層級說明:

M：此項目為強制性(Mandatory)的安全要求。

R：此項為建議(Recommendation)的安全要求。

MC：此項目為強制性(Mandatory)且有條件(Conditional)的安全要求。

RC：此項目為建議(Recommendation)且有條件(Conditional)的安全要求。

(b) 第三欄之條件說明:

(1) 使用通行碼

(2) 使用預設通行碼

(3) 軟體組件不可更新

(4) 受限制設備

(5) 非受限制設備

(6) 收集遙測數據

(7) 基於使用者同意的基礎下處理個人資料

(8) 提供使用者認證的設備

(9) 支援自動更新及/或更新通知的設備

(10) 基於安全起見，設備識別使用硬編碼(hard-coded)唯一性

(11) 更新是透過網路介面傳輸

(12) 有更新機制

(13) 除錯介面是透過實體存取

表 1 安全要求總表

| 安全構面 | 安全要求 | 安全層級與條件 | 安全要求項目 |
|---|---|---|---|
| 5.1 身分鑑別 | 5.1.1 通行碼鑑別 | MC (1) | 5.1.1.1 |
| | | MC (2) | 5.1.1.2 |
| | 5.1.2 身分認證機制 | MC (8) | 5.1.2.1 |
| | | MC (5) | 5.1.2.2 |
| | | M | 5.1.2.3 |
| 5.2 安全漏洞 | 5.2.1 漏洞政策與安全設置 | M | 5.2.1.1 |
| | | R | 5.2.1.2 |
| | | R | 5.2.1.3 |
| | | R | 5.2.1.4 |
| | | R | 5.2.1.5 |
| | | R | 5.2.1.6 |
| | 5.2.2 最小暴露攻擊面 | M | 5.2.2.1 |
| | | M | 5.2.2.2 |
| | | R | 5.2.2.3 |
| | | MC (13) | 5.2.2.4 |
| | | R | 5.2.2.5 |
| | | R | 5.2.2.6 |
| | | R | 5.2.2.7 |
| | | R | 5.2.2.8 |
| | | R | 5.2.2.9 |

| 安全構面 | 安全要求 | 安全層級與條件 | 安全要求項目 |
|---|---|---|---|
| 5.3 軟韌體更新 | 5.3.1 更新安全 | R | 5.3.1.1 |
| | | MC (5) | 5.3.1.2 |
| | | MC (12) | 5.3.1.3 |
| | | RC (12) | 5.3.1.4 |
| | | RC (12) | 5.3.1.5 |
| | | RC (9, 12) | 5.3.1.6 |
| | | MC (12) | 5.3.1.7 |
| | | MC (12) | 5.3.1.8 |
| | | RC (12) | 5.3.1.9 |
| | | M (11, 12) | 5.3.1.10 |
| | | RC (12) | 5.3.1.11 |
| | | RC (12) | 5.3.1.12 |
| | | M | 5.3.1.13 |
| | | RC (3, 4) | 5.3.1.14 |
| | | RC (3, 4) | 5.3.1.15 |
| | | M | 5.3.1.16 |
| 5.4 資料機密性與完整性 | 5.4.1 敏感性安全參數儲存 | M | 5.4.1.1 |
| | | MC (10) | 5.4.1.2 |
| | | M | 5.4.1.3 |
| | | M | 5.4.1.4 |

| 安全構面 | 安全要求 | 安全層級與條件 | 安全要求項目 |
|---|---|---|---|
| 5.4 資料機密性與完整性 | 5.4.2 傳輸資料保護 | M | 5.4.2.1 |
| | | R | 5.4.2.2 |
| | | R | 5.4.2.3 |
| | | R | 5.4.2.4 |
| | | M | 5.4.2.5 |
| | | R | 5.4.2.6 |
| | | M | 5.4.2.7 |
| | | M | 5.4.2.8 |
| 5.5 系統完整性 | 5.5.1 實體入侵防護 | R | 5.5.1.1 |
| | 5.5.2 輸入驗證 | M | 5.5.2.1 |
| 5.6 資源可用性 | 5.6.1 資源管理 | R | 5.6.1.1 |
| | | R | 5.6.1.2 |
| | | R | 5.6.1.3 |
| 5.7 隱私保護 | 5.7.1 隱私保護能力 | R | 5.7.1.1 |
| | | M | 5.7.1.2 |
| | | M | 5.7.1.3 |
| | | M | 5.7.1.4 |
| | | R | 5.7.1.5 |
| | | R | 5.7.1.6 |
| | | R | 5.7.1.7 |
| | | M | 5.7.1.8 |
| | | MC (7) | 5.7.1.9 |

| 安全構面 | 安全要求 | 安全層級與條件 | 安全要求項目 |
|---|---|---|---|
| 5.7 隱私保護 | 5.7.1 隱私保護能力 | M | 5.7.1.10 |
| | | RC (6) | 5.7.1.11 |
| | | MC (6) | 5.7.1.12 |
| 5.8 異常與警示 | 5.8.1 安全事件警示 | R | 5.8.1.1 |
| | | RC (6) | 5.8.1.2 |

### 4.1.1 安全構面：

(a) 身分鑑別：溝通介面須確保鑑別、授權及權限控管相關機制，包括遠端指令管理介面、通訊協定等，應具備一定防護能力，避免遭受蓄意人士入侵。

(b) 漏洞安全：產品之系統、網路服務應防止漏洞及具備即時檢視漏洞之安全機制，及預防與處置機制的資訊安全管理。

(c) 韌體更新：產品之韌體版本更新服務及韌體程式設計等，須具備足夠安全防護。

(d) 資料機密性與完整性：產品傳輸與儲存之資料應具有足夠安全之防護，避免遭受蓄意人士入侵。

(e) 系統完整性：產品測試用連接埠的處置，應具備一定防護能力，視為實體安全要求的標的。

(f) 資源可用性：產品須確保服務可回復正常運作的能力。

(g) 隱私保護：產品須具有個人隱私的保護機制。

(h) 異常與警示：產品於發生安全事件須具有警示能力。

### 4.1.2 安全要求項目：

依安全構面所設計對應之安全要求，其中每一安全要求包含一個或以上之安全要求項目。

# 5. 標準規範

本節詳盡載明消費性物聯網產品為滿足安全要求應採取的方法，消費性物聯網產品符合本節中所有安全基本要求。

## 5.1 身分鑑別

### 5.1.1 通行碼鑑別

5.1.1.1 廠商所生產之裝置，其預設通行碼都應相異；抑或首次成功取得產品存取之授權，應強制更改預設通行碼。

5.1.1.2 當產品採用預設通行碼，通行碼生成機制應足夠隨機，例如:密碼生成採用偽隨機數產生器(Pseudo Random Number Generators, PRNG) 。

### 5.1.2 身分認證機制

5.1.2.1 產品應提供身分認證機制，且使用者可更改或重設身分認證因子，例如:使用者帳號密碼、指紋、智慧卡等。

5.1.2.2 使用者登入介面(包括但不限於 web 介面、API 介面等)之登入輸入頻率與次數限制應：

(a)最高 5 次嘗試登入失敗即鎖定帳戶。

(b)在一定時間內須持續鎖定帳戶。

(c)至少經過一定時間，始可將失敗的登入嘗試計數器重設為 0。

5.1.2.3 產品之身分認證因子傳輸應加密傳輸，加密方式採用 NIST SP 800-140C 所核可同等或以上等級之加密演算法。

## 5.2 漏洞安全

### 5.2.1 漏洞政策與安全設置

5.2.1.1 廠商應提供產品之漏洞揭露政策，政策內容應包括但不限於：

(a)回報漏洞問題之連絡資訊，例如:廠商於使用說明書中提供漏洞回報的專線或 email 信箱。

(b)接收漏洞問題的初始確認程序，例如:漏洞揭露政策中訂定收到漏洞後多久時間內須完成問題確認。

(c)問題處理至問題解決之各階段的狀態更新，例如:廠商可透過與漏洞賞金平台合作，運用平台的漏洞回報與處理流程機制。

5.2.1.2 廠商宜及時處理已揭露的漏洞，例如:漏洞修正計畫載明漏洞風險等級、等級對應之修復處理時間之界定等漏洞處理原則。

5.2.1.3 漏洞揭露政策聲明宜包含維護期間內對其產品之安全漏洞持續監控、識別與修正。

5.2.1.4 在安裝與維護的過程，產品提供予使用者設定的安全性設置，宜符合簡易的安全性設步驟、各步驟的最佳建議有醒目提示、具安全性的預設設定參數，以協助使用者完成最佳安全設置。

5.2.1.5 產品宜提供產品安全設置指南。

5.2.1.6 廠商宜提供如何檢查產品是否具備安全設置的指南。

### 5.2.2 最小暴露攻擊面

5.2.2.1 產品啟用之網路埠與網路服務應為廠商提供必要服務之所需。

5.2.2.2 在初始狀態下，裝置的網路服務所揭露給未認證方的訊息應為廠商提供必要服務之所需。

5.2.2.3 產品啟用之實體介面宜為廠商提供必要服務之所需。

5.2.2.4 產品不應透過實體介面存取產品除錯模式(debug mode)。

5.2.2.5 產品啟用之軟體服務宜為廠商提供必要服務之所需。

5.2.2.6 產品之原始碼宜最小化且為必要功能之所需。

5.2.2.7 確保產品執行所需之特權控制與廠商所宣告的一致，且廠商所宣告的特權控制機制宜滿足職責分離(separation of duty)、需所知(need to know)和最小化特權(minimization of privilege)的原則。

5.2.2.8 產品宜支援硬體等級的記憶體存取控制機制，例如:MMU、MPU 技術進行空間保護。

5.2.2.9 廠商宜提供產品安全開發說明文件，包括但不限於開發人員安全培訓、軟體需求設計階段、安全編碼技術、實施階段的安全收費、安全測試、安全審查、與軟體安全維護有關的資產和資訊的保存、安全部署、安全事件應變流程和管理第三方軟體供應商。

## 5.3 軟韌體更新

### 5.3.1 更新安全

5.3.1.1 產品之所有軟體組件宜具備安全更新功能。

5.3.1.2 當產品為非受限制設備，產品之軟/韌體應具備安全更新功能，更新安全功能包括但不限於防止安裝舊版本、傳輸加密演算法符合 NIST SP 800-140C、更新傳輸走安全通道。

5.3.1.3 當產品支援安全更新機制，應具備簡單易用之軟韌體更新方式，包括但不限於自動更新軟韌體、透過關聯服務啟動更新、透過產品之 web 介面啟動更新。

5.3.1.4 當產品支援安全更新機制，產品宜使用自動軟體更新機制。

5.3.1.5 當產品支援安全更新機制，產品宜於初始化後定期檢查是否有可用更新。

5.3.1.6 當產品支援自動更新、自動更新通知功能，產品宜於初始化後自動啟用更新與更新通知功能，且自動更新與更新通知功能須提供使用者自行設定開啟更新、關閉更新、延遲更新、開啟通知、關閉通知及延遲通知的功能選項。

5.3.1.7 當產品支援安全更新機制，若產品更新路徑通過安全通道，則安全通道版本應符合 TLS v1.2 以上版本，同時金鑰交換協議應支援前向保密，且安全更新機制應採用 NIST SP 800-140C 所核可之密碼演算法。

5.3.1.8 當產品支援安全更新機制，應確保產品能即時安全更新。

5.3.1.9 當產品支援安全更新機制，宜確保更新檔的真實性與完整性，簽章演算法應採用 NIST SP 800-140C 同等或以上強度演算法。

5.3.1.10 當產品支援線上安全更新，產品應鑑別更新伺服器身分之真實性，且應於更新檔傳輸過程中確認真實性與完整性，如使用密碼演算法應採用 NIST SP 800-140C 同等或以上強度演算法。

5.3.1.11 產品宜以清楚識別的方式通知使用者進行更新，且更新資訊宜說明該更新所能緩解的風險，清楚識別的通知方式包括但不限於使用彈跳視窗、推播訊息及電子郵件。

5.3.1.12 當產品支援更新機制，產品更新過程若會中斷產品基本功能，則宜於更新前告知使用者。

5.3.1.13 廠商提供使用者的產品支援期限聲明應淺顯易懂，支援期限聲明公告於包括但不限在產品網站、包裝、使用說明書等。

5.3.1.14 無法軟體更新之受限制設備產品，廠商宜以淺顯易懂的方式說明無法軟體更新之理由、硬體替換的支援期限與方法。

5.3.1.15 無法軟體更新之受限制設備產品，產品宜可被隔離且可替換硬體。

5.3.1.16 產品型號及名稱應標示在包括但不限於產品標籤、實體介面，讓使用者能清楚辨識。

## 5.4 資料機密性與完整性

### 5.4.1 敏感性安全參數儲存

5.4.1.1 產品持久性儲存器(persistent storage)中的敏感性安全參數應加密儲存，或存放於產品的安全區域，從正常作業環境中隔離。

5.4.1.2 當產品出於安全為目的將產品唯一識別碼以硬編碼方式儲存，應防止實體或軟體等方式篡改。

5.4.1.3 產品的關鍵安全參數不應使用於軟體原始碼。

5.4.1.4 產品用於更新及與關聯服務間傳輸所使用之關鍵安全參數應具唯一性，例如:產品金鑰。

## 5.4.2 傳輸資料保護

5.4.2.1 產品之安全傳輸應使用符合國際標準要求或公認之資安產業慣例之最佳傳輸加密技術，例如，安全通道使用 TLS v1.2 以上版本、採用 NIST SP 800-140C 所核可的同等或以上等級之密碼演算法、IPSec、MPLS 等。

5.4.2.2 產品所有之網路與安全功能於交付前宜通過審查(review)或評估(evaluate)，審查內容包括但不限於廠商已識別之資安缺陷及漏洞修補結果，評估內容包括但不限於廠商所識別的必要安全措施及緩解措施。

5.4.2.3 產品之密碼演算法及密碼基元(cryptographic primitives)宜可被更新，或產品為不可更新設備時，產品的建議使用年限不得超過密碼演算法建議使用期限。

5.4.2.4 存取產品資源前，宜透過身分鑑別機制。

5.4.2.5 變更產品安全相關設定之功能應具備身分認證機制，包括但不限於本地端管理介面、實體介面執行通行碼變更或權限變更；若產品使用 ARP、DHCP、DNS、ICMP 和 NTP 不在此限。

5.4.2.6 產品之關鍵安全參數宜加密傳輸，資料保護之加密方式須採用 NIST SP 800-140C 所核可的同等或以上等級之加密演算法。

5.4.2.7 以遠端指令介面傳送關鍵安全參數應加密或使用安全加密通道。

5.4.2.8 廠商應提供關鍵安全參數之安全管理程序說明文件，例如:金鑰管理須符合 NIST SP 800-57[8]的要求。

## 5.5 系統完整性

### 5.5.1 實體入侵防護

5.5.1.1 產品宜支援安全啟動(Secure boot)機制。

### 5.5.2 輸入驗證

5.5.2.1 產品之使用者介面應驗證輸入的語法和內容，包括但不限於本地端管理介面、網路服務介面、應用程式介面(APIs)。

## 5.6 資源可用性

### 5.6.1 資源管理

5.6.1.1 針對網路和電源中斷的情況，產品宜設置因應網路和電源中斷的彈性機制，例如:設置備用電源、資料即時備份等。

5.6.1.2 產品宜在網路中斷時仍可保持本地端運作，且在網路恢復後，產品能回復正常運作。

5.6.1.3 產品宜具備保持連線穩定與功能正常運作之能力，包括但不限於產品分批線上更新、產品於恢復網路連線時隨機依序連線。

## 5.7 隱私保護

### 5.7.1 隱私保護能力

5.7.1.1 產品之個人資料宜加密傳輸，保護資料的加密方式須採用 NIST SP 800-140C 所核可之同等或以上之加密演算法。

5.7.1.2 產品之敏感性個人資料應加密傳輸，保護資料的加密方式須採用 NIST SP 800-140C 所核可之同等或以上之加密演算法。

5.7.1.3 產品若有外部感測功能應清楚告知使用者，告知方式包括但不限於記載於產品使用說明書、產品包裝等。

5.7.1.4 產品應提供使用者簡便的功能以刪除使用者資料(user data)，例如:使用者友善介面且操作步驟盡可能減少至必要的步驟。

5.7.1.5 產品宜提供使用者簡便的功能以刪除儲存於關聯服務中的個人資料。

5.7.1.6 產品宜提供使用者明確的刪除個人資料之方法說明，例如:產品使用手冊中說明刪除使用者資料的功能和方法。

5.7.1.7 廠商所提供之刪除個人資料機制，從產品、關聯服務、應用程式完成刪除後須明確告知使用者刪除狀態。

5.7.1.8 廠商應具備對於收集、利用、處理使用者個人資料的管理機制，管理機制適用於包括但不限於產品開發商、系統整合商、第三方廠商和廣告商。

5.7.1.9 廠商應具備使用者個人資料之使用授權機制，在收集、利用、處理使用者個人資料前應由經使用者同意。

5.7.1.10 廠商應提供使用者個人資料使用授權之撤銷機制。

5.7.1.11 產品所收集之遙測數據若包含個人資料時，該個人資料之內容宜為廠商必要之所需，包括但不限於產品開發商、系統整合商、第三方廠商和廣告商。

5.7.1.12 產品所收集之遙測數據，應提供說明遙測數據之種類、使用目的，遙測數據使用者包括但不限於產品開發商、系統整合商、第三方廠商和廣告商。

## 5.8 異常警示

### 5.8.1 安全事件警示

5.8.1.1 當偵測到產品有未經授權的軟體變更時，產品宜向管理者或使用者發出警示。

5.8.1.2 產品所收集之遙測數據宜檢查是否存在安全異常，以作為監控安全事件之用途。

# 附錄 A
# (規定)
# 安全通道版本使用要求

指超文本傳輸協定(HTTP)結合安全套接層協定(SSL)或傳輸層安全性協定(TLS)，建立安全通道以保護傳輸中資料不被竊取之技術；然而安全套接層協定在 2014 年 10 月由 Google 指出其資訊安全漏洞，宣布將全面禁用，所以已經完全由傳輸層安全性協定取代安全套接層協定。但傳輸層安全性協定 v1.0 存在可以降級到安全套接層協定 v3.0 的功能，使得傳輸層安全性協定 v1.0 同樣不被信任，因此目前本標準應使用的版本為：傳輸層安全性協定 v1.2 同等或以上之版本。

# 附錄 B
# (參考)
# 安全要求事項與各標準規範對照表

本標準與 ETSI EN 303 645 之比對結果，如下表所示：

表 B.1 安全要求事項與各標準規範對照表

| 對應標準規範 | | |
|---|---|---|
| 本標準要求事項 | | ETSI EN 303 645 |
| 5.1.1.1 | 廠商所生產之裝置，其預設通行碼都應相異；抑或首次成功取得產品存取之授權，應強制更改預設通行碼。 | 5.1-1 |
| 5.1.1.2 | 當產品採用預設通行碼，通行碼生成機制應足夠隨機，例如:密碼生成採用偽隨機數產生器度(PRNG) 。 | 5.1-2 |
| 5.1.2.1 | 產品應提供身分認證機制，且使用者可更改或重設身分認證因子，例如:使用者帳號密碼、指紋、智慧卡等。 | 5.1-4 |
| 5.1.2.2 | 使用者登入介面(包括但不限於 web 介面、API 介面等)之登入輸入頻率與次數限制應：<br>(a)最高 5 次嘗試登入失敗即鎖定帳戶。<br>(b)在一定時間內須持續鎖定帳戶。<br>(c)至少經過一定時間，始可將失敗的登入嘗試計數器重設為 0。 | 5.1-5 |
| 5.1.2.3 | 產品之身分認證因子傳輸須加密傳輸，加密方式採用 NIST SP 800-140C 所核可同等或以上等級之加密演算法。 | 5.1-3 |
| 5.2.1.1 | 廠商應提供產品之漏洞揭露政策，政策內容應包括但不限於： | 5.2-1 |

| 對應標準規範 | | |
|---|---|---|
| | 本標準要求事項 | ETSI EN 303 645 |
| | (a)回報漏洞問題之連絡資訊。例如:廠商於使用說明書中提供漏洞回報的專線或 email 信箱。<br>(b)接收漏洞問題的初始確認程序。例如:漏洞揭露政策中訂定收到漏洞後多久時間內須完成問題確認。<br>(c)問題處理至問題解決之各階段的狀態更新。例如:廠商可透過與漏洞賞金平台合作，運用平台的漏洞回報與處理流程機制。 | |
| 5.2.1.2 | 廠商宜及時處理已揭露的漏洞，例如:漏洞修正計畫載明漏洞風險等級、等級對應之修復處理時間之界定等漏洞處理原則。 | 5.2-2 |
| 5.2.1.3 | 漏洞揭露政策聲明宜包含維護期間內對其產品之安全漏洞持續監控、識別與修正。 | 5.2-3 |
| 5.2.1.4 | 在安裝與維護的過程，產品的提供予使用者設定的安全性設置，宜符合簡易的安全性設步驟、各步驟的最佳建議有醒目提示、具安全性的預設設定參數，以協助使用者完成最佳安全設置。 | 5.12-1 |
| 5.2.1.5 | 產品宜提供產品安全設置指南。 | 5.12-2 |
| 5.2.1.6 | 廠商宜提供檢查產品是否具備安全設置的指南。 | 5.12-3 |
| 5.2.2.1 | 產品啟用之網路埠與網路服務應為廠商提供必要服務之所需。 | 5.6-1 |
| 5.2.2.2 | 在初始狀態下，裝置的網路服務所揭露給未認證方的訊息應為廠商提供必要服務之所需。 | 5.6-2 |
| 5.2.2.3 | 產品啟用之實體介面宜為廠商提供必要服務之所需。 | 5.6-3 |

| 對應標準規範 | | |
|---|---|---|
| 本標準要求事項 | | ETSI EN 303 645 |
| 5.2.2.4 | 產品不得透過實體介面存取產品除錯模式(debug mode)。 | 5.6-4 |
| 5.2.2.5 | 產品啟用之軟體服務宜為廠商提供必要服務之所需。 | 5.6-5 |
| 5.2.2.6 | 產品之原始碼宜最小化且為必要功能之所需。 | 5.6-6 |
| 5.2.2.7 | 確保產品執行所需之特權控制與廠商所宣告的一致，且廠商所宣告的特權控制機制宜滿足職責分離(separation of duty)、需所知(need to know)和最小化特權(minimization of privilege)的原則。 | 5.6-7 |
| 5.2.2.8 | 產品宜支援硬體等級的記憶體存取控制機制，例如:MMU、MPU 技術進行空間保護。 | 5.6-8 |
| 5.2.2.9 | 廠商宜提供產品安全開發說明文件，包括但不限於開發人員安全培訓、軟體需求設計階段、安全編碼技術、實施階段的安全收費、安全測試、安全審查、與軟體安全維護有關的資產和資訊的保存、安全部署、安全事件應變流程和管理第三方軟體供應商。 | 5.6-9 |
| 5.3.1.1 | 產品之所有軟體組件宜具備安全更新功能。 | 5.3-1 |
| 5.3.1.2 | 當產品為非受限制設備，產品之軟/韌體應具備安全更新功能，更新安全功能包括但不限於防止安裝舊版本、傳輸加密演算法符合 NIST SP 800-140C、更新傳輸走安全通道。 | 5.3-2 |
| 5.3.1.3 | 當產品支援安全更新機制，應具備簡單易用之軟韌體更新方式，包括但不限於自動更新軟韌體、透過關聯服務啟動更新、透過產品之 web 介面啟動更新。 | 5.3-3 |

| 對應標準規範 | | |
|---|---|---|
| 本標準要求事項 | | ETSI EN 303 645 |
| 5.3.1.4 | 當產品支援安全更新機制，產品宜使用自動軟體更新機制。 | 5.3-4 |
| 5.3.1.5 | 當產品支援安全更新機制，產品宜於初始化後定期檢查是否有可用更新。 | 5.3-5 |
| 5.3.1.6 | 當產品支援自動更新、自動更新通知功能，產品宜於初始化後自動啟用更新與更新通知功能，且自動更新與更新通知功能須提供使用者自行設定開啟更新、關閉更新、延遲更新、開啟通知、關閉通知及延遲通知的功能選項。 | 5.3-6 |
| 5.3.1.7 | 當產品支援安全更新機制，若產品更新路徑通過安全通道，則安全通道版本應符合 TLS v1.2 以上版本，同時金鑰交換協議應支援前向保密，且安全更新機制應採用 NIST SP 800-140C 所核可之密碼演算法。 | 5.3-7 |
| 5.3.1.8 | 當產品支援安全更新機制，應確保產品能即時安全更新。 | 5.3-8 |
| 5.3.1.9 | 當產品支援安全更新機制，宜確保更新檔的真實性與完整性，簽章演算法應採用 NIST SP 800-140C 同等或以上強度演算法。 | 5.3-9 |
| 5.3.1.10 | 當產品支援線上安全更新，產品應鑑別更新伺服器身分之真實性，且應於更新檔傳輸過程中確認真實性與完整性，如使用密碼演算法應採用 NIST SP 800-140C 同等或以上強度演算法。 | 5.3-10 |
| 5.3.1.11 | 產品宜以清楚識別的方式通知使用者進行更新，且更新資訊宜說明該更新所能緩解的風險，清楚識別的通知方式包括但不限於使用彈跳視窗、推播訊息及電子郵件。 | 5.3-11 |

| 對應標準規範 | | |
|---|---|---|
| 本標準要求事項 | | ETSI EN 303 645 |
| 5.3.1.12 | 當產品支援更新機制，產品更新過程若會中斷產品基本功能，則宜於更新前告知使用者。 | 5.3-12 |
| 5.3.1.13 | 廠商提供使用者的產品支援期限聲明應淺顯易懂，支援期限聲明公告於包括但不限在產品網站、包裝、使用說明書等。 | 5.3-13 |
| 5.3.1.14 | 無法軟體更新之受限制設備產品，廠商宜以淺顯易懂的方式說明無法軟體更新之理由、硬體替換的支援期限與方法。 | 5.3-14 |
| 5.3.1.15 | 無法軟體更新之受限制設備產品，產品宜可被隔離且可替換硬體。 | 5.3-15 |
| 5.3.1.16 | 產品型號及名稱應標示在包括但不限於產品標籤、實體介面，讓使用者能清楚辨識。 | 5.3-16 |
| 5.4.1.1 | 產品持久性儲存器(persistent storage)中的敏感性安全參數應加密儲存，或存放於產品的安全區域，從正常作業環境中隔離。 | 5.4-1 |
| 5.4.1.2 | 當產品出於安全為目的將產品唯一識別碼以硬編碼方式儲存，應防止實體或軟體等方式篡改。 | 5.4-2 |
| 5.4.1.3 | 產品的關鍵安全參數不應使用於軟體原始碼。 | 5.4-3 |
| 5.4.1.4 | 產品用於更新及與關聯服務間傳輸所使用之關鍵安全參數應具唯一性，例如:產品金鑰。 | 5.4-4 |
| 5.4.2.1 | 產品之安全傳輸應使用符合國際標準要求或公認之資安產業慣例之最佳傳輸加密技術，例如，安全通道使用 TLS v1.2 以上版本、採用 NIST SP 800-140C 所核可的同等或以上等級之密碼演算法、IPSec、MPLS 等。 | 5.5-1 |
| 5.4.2.2 | 產品所有之網路與安全功能於交付前宜通過審查(review)或評估(evaluate)，審查內容包括但不限於 | 5.5-2 |

| 對應標準規範 | | |
|---|---|---|
| 本標準要求事項 | | ETSI EN 303 645 |
| | 廠商已識別之資安缺陷及漏洞修補結果，評估內容包括但不限於廠商所識別的必要安全措施及緩解措施。 | |
| 5.4.2.3 | 產品之密碼演算法及密碼基元(cryptographic primitives)宜可被更新，或產品為不可更新設備時，產品的建議使用年限不得超過密碼演算法建議使用期限。 | 5.5-3 |
| 5.4.2.4 | 存取產品資源前，宜透過身分鑑別機制。 | 5.5-4 |
| 5.4.2.5 | 變更產品安全相關設定之功能應具備身分認證機制，包括但不限於本地端管理介面、實體介面執行通行碼變更或權限變更；若產品使用 ARP、DHCP、DNS、ICMP 和 NTP 不在此限。 | 5.5-5 |
| 5.4.2.6 | 產品之關鍵安全參數宜加密傳輸，資料保護之加密方式須採用 NIST SP 800-140C 所核可的同等或以上等級之加密演算法。 | 5.5-6 |
| 5.4.2.7 | 以遠端指令介面傳送關鍵安全參數應加密或使用安全加密通道。 | 5.5-7 |
| 5.4.2.8 | 廠商應提供關鍵安全參數之安全管理程序說明文件，例如:金鑰管理須符合 NIST SP 800-57 的要求。 | 5.5-8 |
| 5.5.1.1 | 產品宜支援安全啟動(Secure boot)機制。 | 5.7-1 |
| 5.5.2.1 | 產品之使用者介面應驗證輸入的語法和內容，包括但不限於本地端管理介面、網路服務介面、應用程式介面(APIs)。 | 5.13-1 |

| 對應標準規範 | | |
|---|---|---|
| 本標準要求事項 | | ETSI EN 303 645 |
| 5.6.1.1 | 針對網路和電源中斷的情況，產品宜設置因應網路和電源中斷的彈性機制，例如:設置備用電源、資料即時備份等。 | 5.9-1 |
| 5.6.1.2 | 產品宜在網路中斷時仍可保持本地端運作，且在網路恢復後，系統能回復正常運作。 | 5.9-2 |
| 5.6.1.3 | 產品宜具備保持連線穩定與功能正常運作之能力，包括但不限於產品分批線上更新、產品於恢復網路連線時隨機依序連線。 | 5.9-3 |
| 5.7.1.1 | 產品之個人資料宜加密傳輸，保護資料的加密方式須採用 NIST SP 800-140C 所核可之同等或以上之加密演算法。 | 5.8-1 |
| 5.7.1.2 | 產品之敏感性個人資料應加密傳輸，保護資料的加密方式須採用 NIST SP 800-140C 所核可之同等或以上之加密演算法。 | 5.8-2 |
| 5.7.1.3 | 產品若有外部感測功能應清楚告知使用者，告知方式包括但不限於記載於產品使用說明書、產品包裝等。 | 5.8-3 |
| 5.7.1.4 | 產品應提供使用者簡便的功能以刪除使用者資料，例如:使用者友善介面且操作步驟盡可能減少至必要的步驟。 | 5.11-1 |
| 5.7.1.5 | 產品宜提供使用者簡便的功能以刪除儲存於關聯服務中的個人資料。 | 5.11-2 |
| 5.7.1.6 | 產品宜提供使用者明確的刪除個人資料之方法說明，例如:產品使用手冊中說明刪除使用者資料的功能和方法。 | 5.11-3 |

| 對應標準規範 | | |
|---|---|---|
| 本標準要求事項 | | ETSI EN 303 645 |
| 5.7.1.7 | 廠商所提供之刪除個人資料機制，從產品、關聯服務、應用程式完成刪除後須明確告知使用者刪除狀態。 | 5.11-4 |
| 5.7.1.8 | 廠商應具備對於收集、利用、處理使用者個人資料的管理機制，管理機制適用於包括但不限於產品開發商、系統整合商、第三方廠商和廣告商。 | 6.1 |
| 5.7.1.9 | 廠商應具備使用者個人資料之使用授權機制，在收集、利用、處理使用者個人資料前應由經使用者同意。 | 6.1 |
| 5.7.1.10 | 廠商應提供使用者個人資料使用授權之撤銷機制。 | 6.1 |
| 5.7.1.11 | 產品所收集之遙測數據若包含個人資料時，該個人資料之內容宜為廠商必要之所需，包括但不限於產品開發商、系統整合商、第三方廠商和廣告商。 | 6.1 |
| 5.7.1.12 | 產品所收集之遙測數據，應提供說明遙測數據之種類、使用目的，遙測數據使用者包括但不限於產品開發商、系統整合商、第三方廠商和廣告商。 | 6.1 |
| 5.8.1.1 | 當偵測到產品有未經授權的軟體變更時，產品宜向管理者或使用者發出警示。 | 5.7-2 |
| 5.8.1.2 | 產品所收集之遙測數據宜檢查是否存在安全異常，以作為監控安全事件之用途。 | 5.10-1 |

# 參考資料

(1) IEK 物聯網資安威脅與解決方案發展方向, https://ieknet.iek.org.tw/iekppt/ppt_more.aspx?actiontype=ppt&indu_idno=14&domain=44&sld_preid=4997

(2) ETSI TS 103 645 V1.1.1 (2019-02), CYBER; Cyber Security for Consumer Internet of Things.

(3) IEC 62443-4-2-2018 Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components.

(4) NISTIR 8259 Draft (2nd) Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline.

(5) NIST, National Vulnerability Database, https://nvd.nist.gov/vuln/full-listing

(6) National Institute of Standards and Technology, NIST SP 800-140C, CMVP Approved Security Functions, available at URL: https://csrc.nist.gov/projects/cryptographic-module-validation-program

(7) FIRST, Common Vulnerability Scoring System version 3.1: Specification Document, https://www.first.org/cvss/specification-document

(8) NIST Special Publication 800-57: Recommendation for Key Management, https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

# 版本修改紀錄

| 版本 | 時間 | 摘要 |
|---|---|---|
| v1.0 | 2021/11/25 | 出版 |
| | | |
| | | |
| | | |
| | | |


地　址・台北市中正區北平東路30-2號6樓
電　話・+886-2-23567698
Email・secretariat@taics.org.tw
www.taics.org.tw